HW

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/878,319	06/12/2001	Mark Crosbie	10004512-1	2127

7590 12/13/2005

EXAMINER	
PARTHASARATHY, PRAMILA	
ART UNIT	PAPER NUMBER
2136	

IP Administration
Legal Department, M/S 35
HEWLETT-PACKARD COMPANY
P.O. Box 272400
Fort Collins, CO 80528-9599

DATE MAILED: 12/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/878,319	CROSBIE ET AL.	
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 September 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-48* is/are pending in the application.

4a) Of the above claim(s) *11,33,34 and 44-48* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10,12-32 and 35-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. In view of the Appeal Brief filed on 9/20/2005, PROSECUTION IS HEREBY REOPENED. Applicant's arguments with respect to claims 1 – 10, 12 – 32 and 35 – 43 have been considered but are moot in view of the new ground(s) of rejection as set forth below.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

2. Claims 1 – 10, 12 – 32 and 35 – 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moran (U.S. Patent Number 6,647,400) in view of Kuznetsov et al. (U.S. Patent Number 5,483,649).

3. Regarding Claim 1, Moran teaches

reading kernel records (Column 7 line 39 – Column 8 line 20 and Column 11 lines 15 – 54);

reformatting each of the read kernel records into a different format, wherein the different format is a memory mapped file (Column 9 line 54 – Column 10 line 32, Column 27 lines 37 – 39 and Column 29 lines 4 – 52);

parsing the records and comparing the parsed records against one or more templates (Column 18 lines 6 – 58).

Moran does not explicitly discloses reformatting each of the record kernel records into a different format, wherein the different format is a memory mapped file (Moran discloses converting kernel records into a different format. However, Kuznetsov discloses a system of protecting data stored on the hard disk from an inadvertent or intentional distortion, wherein the OS kernel-level request check program reformats kernel records into a different format (Kuznetsov Column 11 line 42 – Column 12 line 38). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to reformat each kernel record into a different format. One of ordinary skill in the art would have been motivated to do this because it would create flexibility to read the file on different systems.

4. Regarding Claim 29, Moran teaches

monitoring a predetermined set of files for modifications (Column 8 lines 6 – Column 10 line 55 and Column 11 lines 16 – 54);

monitoring a predetermined set of directories for modifications (Column 8 line 6 – Column 10 line 55 and Column 11 lines 16 – 54);

generating an alert for each occurrence of a modification of a monitored file, wherein if a directory is specifically excluded and a file in the specifically excluded directory is specifically included the file is monitored, and wherein the predetermined set of files includes a system kernel file and system kernel configuration files (Column 10 lines 14 – 55; Column 13 lines 1 – 31 and Column 35 lines 9 – 42); and

generating an alert for each occurrence of a modification of a monitored directory (Column 10 lines 14 – 55; Column 13 lines 1 – 31, Column 32 line 44 – Column 33 line 62 and Column 35 lines 9 – 42).

Moran does not explicitly discloses reformatting each of the record kernel records into a different format, wherein the different format is a memory mapped file (Moran discloses converting kernel records into a different format. However, Kuznetsov discloses a system of protecting data stored on the hard disk from an inadvertent or intentional distortion, wherein the OS kernel-level request check program reformats kernel records into a different format (Kuznetsov Column 11 line 42 – Column 12 line 38). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to reformat each kernel record into a different format. One of

ordinary skill in the art would have been motivated to do this because it would create flexibility to read the file on different systems.

5. Claim 2 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches wherein the kernel audit logs includes information about each system call (Column 8 line 6 – 46 and Column 9 lines 12 – 65).

6. Claim 4 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches monitoring system log files (Column 10 lines 14 – 55).

7. Claim 5 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches comprising a system call (Column 10 lines 33 – 47).

8. Claim 6 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches wherein the system call was initiated by a library call (Column 10 lines 33 – 47 and Column 13 lines 1 – 11).

9. Claim 8 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches comprising determining that an intrusion has occurred and generating an alert message (Column 8 lines 6 – 46).

10. Claim 9 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches comprising encrypting information sent between the host-based intrusion system and a network (Column 16 lines 15 – 29).

11. Claim 10 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches comprising displaying an alert message that an intrusion has occurred (Column 8 lines 6 – 46 and Column 10 lines 14 – 55).

12. Claim 14 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches wherein the one or more templates is a modification of files/directories template (Column 18 lines 6 – 58 and Column 31 lines 31 – 40).

13. Claim 15 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches wherein the one or more templates is a change to log files template (Column 2 lines 40 – 47; Column 10 lines 14 – 55 and Column 11 lines 41 – 54).

14. Claim 16 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches wherein the one or more templates is a SetUID files template (Column 9 lines 33 – 47 and Column 12 lines 46 – 67).

15. Claim 17 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches wherein the one or more templates is a creation of world-writables template (Column 11 line 55 – Column 12 line 67).

16. Claim 18 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches wherein the one or more templates is a repeated failed logins template (Column 19 line 49 – Column 20 line 67).

17. Claim 19 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches wherein the one or more templates is a repeated failed SU commands template (Column 23 lines 14 – 46 and Column 25 lines 15 – 45).

18. Claim 20 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches wherein the one or more templates is a race conditions attack template (Column 12 lines 31 – 67).

19. Claim 21 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches wherein the one or more templates is a buffer overflow attacks template (Column 9 lines 33 – 47 and Column 33 line 64 – Column 34 line 42).

20. Claim 22 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches wherein the one or more templates is a modification of another user's file template (Column 18 lines 6 – 58 and Column 31 lines 31 – 40).

21. Claim 23 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches wherein one or more templates is a monitor for the start of interactive sessions template (Column 38 lines 31 – 51).

22. Claim 24 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches wherein the one or more template is a monitor logins/logouts template (Column 23 lines 14 – 46 and Column 24 lines 33 – 41).

23. Claim 25 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches wherein the one or more templates is chosen from the group including:

a modification of files/directories template (Column 18 lines 6 – 58 and Column 31 lines 31 – 40);

a change to log files template (Column 2 lines 40 – 47; Column 10 lines 14 – 55 and Column 11 lines 41 – 54);

a SetUID files template (Column 9 lines 33 – 47 and Column 12 lines 46 – 67);

a creation of world-writables template (Column 11 line 55 – Column 12 line 67);

a repeated failed logins template (Column 19 line 49 – Column 20 line 67);

a repeated failed SU commands template (Column 23 lines 14 – 46 and Column 25 lines 15 – 45);

a race conditions attack template (Column 12 lines 31 – 67);

a buffer overflow attacks template (Column 9 lines 33 – 47 and Column 33 line 64 – Column 34 line 42);

a modification of another user's file template (Column 18 lines 6 – 58 and Column 31 lines 31 – 40);

a monitor for the start of interactive sessions template (Column 38 lines 31 – 51); and

a monitor logins/logouts template (Column 23 lines 14 – 46 and Column 24 lines 33 – 41).

24. Claim 26 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches wherein the kernel records are read from different computers (Moran Column 10 lines 14 – 55 and Column 17 line 50 – Column 18 line 5; Kuznetsov Column 11 line 42 – Column 12 line 38).

25. Claim 27 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches wherein parsed records are compared against the one or more templates using at least one correlator (Column 11 lines 16 – 28; Column 23 lines 14 – 46 and Column 24 lines 47 – 51).

26. Claim 28 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches wherein said parsing step compares the parsed records against one or more templates simultaneously (Column 32 line 44 – Column 33 line 11).

27. Claim 30 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches determining which files to monitor of all files on a computer to form the predetermined set of files; determining which directories to monitor of all directories on a computer to form the predetermined set of directories (Column 8 lines 6 – 46; Column 11 line 16 – Column 12 line 30; Column 23 lines 14 – 46 and Column 32 line 44 – Column 33 line 62).

28. Claim 31 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches for each said determining step, specifically including a file or directory, specifically excluding a file or directory or not specifically including or excluding a file or directory (Column 8 lines 6 – 46; Column 11 line 16 – Column 12 line 30; Column 23 lines 14 – 46 and Column 32 line 44 – Column 33 line 62).

29. Claim 32 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches wherein a file or directory which is not specifically included or excluded is monitored (Column 8 lines 6 – 46; Column 11 line 16 – Column 12 line 30; Column 23 lines 14 – 46 and Column 32 line 44 – Column 33 line 62).

30. Claim 35 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches wherein the predetermined set of files includes /stand/vmunix, /stand/kernel and stand/bootconf (Column 32 line 44 – Column 33 line 62).

31. Claim 36 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches wherein the predetermined set of files includes files defining the users on a system and files used to create accounts (Column 11 line 55 – Column 12 line 30; Column 20 lines 36 – 67 and Column 25 line 15 – Column 26 line 45).

32. Claim 37 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches wherein the predetermined set of files includes /etc/passwd and /etc/group (Column 11 line 55 – Column 12 line 30; Column 20 lines 36 – 67 and Column 32 line 49 – Column 33 line 11).

33. Claim 38 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches wherein the predetermined set of files includes files which control what network services are running and which controls programs used to fulfill service requests (Column 19 lines 28 – 65 and Column 21 line 1 – 14).

34. Claim 39 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches wherein the predetermined set of files includes /etc/inetd.conf (Column 11 line

55 – Column 12 line 30; Column 20 lines 36 – 67 and Column 32 line 49 – Column 33 line 11).

Claim 40 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches wherein the predetermined set of files includes files which are used to control the remote access of the user root without requiring a password (Column 23 lines 14 – 46 and Column 35 lines 9 – 63).

35. Claim 41 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches wherein the predetermined set of files includes/.rhosts and /.shosts (Column 9 lines 1 – 22 and Column 35 lines 9 – 63).

36. Claim 42 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches wherein the set of files specifically excluded includes temporary files created by a program view (Column 27 line 32 – Column 29 line 52).

37. Claim 43 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches wherein the predetermined set of directories includes Jbin, /sbin and /usr/bin (Column 36 line 7 – Column 37 line 7 and Column 39 lines 43 – 65).

38. Claim 3 is rejected as applied above in rejecting Claim 2. Furthermore, Moran teaches wherein the kernel audit logs includes information about each system call (Column 8 line 6 – 46 and Column 9 lines 12 – 47).

39. Claim 13 is rejected as applied above in rejecting Claim 2. Furthermore, Moran teaches converting the kernel records into an ASCII format for comparison against the one or more templates (Column 10 lines 14 – 53; Column 11 lines 29 – 40 and Column 13 lines 26 – 31).

Conclusion

40. Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

41. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

Applicant is urged to consider the references. However, the references should be evaluated by what they suggest to one versed in the art, rather than by their specific disclosure. If applicants are aware of any better prior art than those are cited, they are required to bring the prior art to the attention of the examiner.

42. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m.. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Cel
Primary Examiner
AU2131
12/9/05

Pramila Parthasarathy
December 05, 2005.